



Laureate International Universities

Escuela Superior Politécnica

# MÁSTER OFICIAL EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

## El nuevo Espacio Europeo de Educación Superior

El proceso Bolonia por fin ha llegado a España. Este proceso supone el cambio de un sistema de educación superior español a un **Espacio Europeo de Educación Superior (EEES)**.

Este EEES implica que en el año 2010 las titulaciones universitarias de todos los países europeos garantizarán programas académicos convergentes, lo que significa un reconocimiento inmediato de los títulos en cualquier lugar de Europa, la movilidad entre países, y el aprendizaje continuo.

Las Titulaciones Oficiales se estructurarán en estudios de Grado y de Postgrado; por tanto los títulos de Postgrado Oficial, ya en marcha, se enmarcan en este Espacio Europeo de Educación Superior (EEES).

Los estudios de Postgrado Oficial se dividen en estudios de 2º Ciclo y estudios de 3er Ciclo. En el 2º Ciclo se cursan **Másteres Oficiales** (de uno o dos años de duración) y en el 3er Ciclo el **Doctorado**.

Esta nueva estructura de educación superior por fin permite a los antiguos diplomados e ingenieros o arquitectos técnicos, acceder al Doctorado (3er ciclo) a través de un Máster Oficial.

Los Másteres Oficiales permiten continuar la formación y especializarse en lo que las empresas demandan a día de hoy, con un título oficial que es válido en cualquier país europeo, y convalidable en cualquier otro país.

## La Universidad Europea de Madrid garantiza la máxima profesionalidad en la formación de postgrado

La Universidad Europea de Madrid ofrece para el curso 2008/2009: 27 Másteres Oficiales, 13 Doctorados y más de 60 títulos propios de postgrado. Para la concepción y diseño de estos programas, la Universidad analiza cuáles son las necesidades formativas actuales de las empresas, apostando por tres pilares fundamentales:

### Orientación profesional

Todos los cursos de postgrado tienen un denominador común: la participación directa de empresas, instituciones y profesionales de reconocido prestigio en sus respectivos sectores, en el diseño y ejecución de los planes de estudios. La mejor acreditación del estudiante para su incorporación o promoción laboral, la aportan todas las empresas que avalan a la Universidad Europea de Madrid.

### Calidad y diferenciación

La calidad y diferenciación de los postgrados viene marcada por la perfecta combinación de un programa totalmente actualizado, unas excelentes instalaciones donde poder ejercer las prácticas necesarias y, en definitiva, una garantía de profesionalización del alumno.

### Oficialidad y garantía formativa

Por su condición de universidad ofrece postgrados oficiales añadiendo una perspectiva internacional y un profundo vínculo con las profesiones y las empresas de renombre, características propias de la Universidad Europea de Madrid, que abrirán las puertas de futuro a los alumnos.

# MÁSTER OFICIAL EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

El **Máster Oficial en Seguridad de las Tecnologías de la Información y las Comunicaciones** responde a la creciente necesidad y relevancia de la seguridad en el ámbito de las TIC y tiene como objetivo formar **especialistas en seguridad** que combinen una doble vertiente estratégica y técnica.

El Máster proporciona los conocimientos técnicos que fundamentan **las soluciones informáticas** a los requisitos de seguridad en el tratamiento de la información. En cuanto a la vertiente estratégica, se pretende formar a los **responsables de la seguridad empresarial**, proporcionándoles un conocimiento del marco legal, de las necesidades de seguridad en el tratamiento automatizado de la información y de las soluciones disponibles actualmente.

El permanente contacto con las empresas del sector hace que el alumno, una vez finalizado el Máster, **esté preparado para dictar la política de seguridad empresarial** en el tratamiento automatizado de la información y **tenga una posición de empleabilidad preferente** en el área de la gestión de la seguridad y los servicios de consultoría.

El perfil competencial que se promoverá es el siguiente:

- Capacidad de análisis de situaciones problemáticas
- Creatividad y síntesis de soluciones combinando ingredientes heterogéneos
- Planificación en la resolución de problemas técnicos
- Capacidad de anticipación al surgimiento de los problemas mediante un diagnóstico multidisciplinar
- Elaboración de directrices y políticas de seguridad que garanticen los requerimientos de seguridad de las operaciones de tratamiento informatizado de la información.

El programa del Máster cubre los contenidos de las certificaciones más demandadas en la actualidad en relación a la Seguridad de las TIC: **Certified Information Security Manager (CISM) y Certified Information Systems Security Professional (CISSP)**. De esta forma, se facilita el acceso a los estudiantes a dichas certificaciones una vez finalizado el Máster. Además de los contenidos teóricos, las prácticas en laboratorio y el proyecto fin de Máster, el programa incluye conferencias y visitas a empresas del sector, y contempla la posibilidad de que los estudiantes que así lo deseen realicen prácticas remuneradas en algunas de las empresas colaboradoras en el Máster.

El alumno dispondrá del uso del **Campus Virtual** (la plataforma Web educativa de la Universidad) a través del cual podrá enviar sus trabajos y aclarar dudas con profesores del Máster.

## DIRIGIDO A

Ingenieros, Ingenieros Técnicos en Informática o Telecomunicaciones y Licenciados en Ciencias.

Profesionales del sector con titulación universitaria.

## DIRECCIÓN DEL MÁSTER

### D<sup>a</sup>. María Teresa Villalba de Benito

Coordinadora de Infraestructuras Informáticas  
Escuela Superior Politécnica de la Universidad Europea de Madrid

### D. Carlos Jiménez Suárez

Presidente de Secuware  
Master Honoris Causa por IEDE Business School

## DURACIÓN, HORARIO Y LUGAR

### Duración:

#### De octubre 2008 a julio 2009.

El Máster tiene una duración de 386 horas presenciales (60 créditos ECTS) que incluyen 100 horas de prácticas en laboratorios.

El alumno interesado en desarrollar su capacidad investigadora deberá cursar de forma adicional 12 ECTS como complementos de acceso al Doctorado.

### Horario:

Horario *executive*: viernes de 18:00 h. a 22:00 h. y sábados, de 8:30 h. a 16:30 h.

Algunas visitas a empresas podrían realizarse fuera de este horario por motivos de organización (se avisará a los alumnos con suficiente antelación).

### Lugar:

Las clases se imparten en las aulas y laboratorios del Campus La Moraleja. Avda de Bruselas 14.  
28108 Alcobendas. Madrid

Algunas clases puntuales se impartirán en las instalaciones del Campus de Villaviciosa de Odón.

## FORMACIÓN PRÁCTICA

### Laboratorio (100 horas):

- Configuración segura de sistemas Windows
- Configuración segura de sistemas Linux
- Configuración segura de redes inalámbricas
- Configuración segura de servidores de correo
- Instalación y configuración cortafuegos
- Utilización de herramientas de seguridad
- Prácticas de verificaciones de seguridad
- Prácticas de inspección de seguridad

### Prácticas y visitas

Durante el curso se realizarán visitas a las empresas colaboradoras del Programa donde se mostrarán las tecnologías y procedimientos que utilizan en la práctica.

Existe la posibilidad de que alumnos realicen prácticas remuneradas en alguna de las empresas colaboradoras del Programa, según sus necesidades.

Si el profesional tiene experiencia demostrada, las prácticas pueden convalidarse.

## PROGRAMA ACADÉMICO

Los contenidos del programa atienden a las necesidades transmitidas directamente a la Universidad Europea de Madrid por las empresas líderes del sector.

### FORMACIÓN TEÓRICO-PRÁCTICA

#### 1. Arquitecturas y modelos de seguridad de la información

- Principios fundamentales de la seguridad de las Tecnologías de la Información y las Comunicaciones
- Modelos de seguridad
- Las normas y estándares más relevantes en la actualidad
- Los criterios y mecanismos de evaluación y certificación de la seguridad vigente

#### 2. Políticas de seguridad

- Principios por los que se rige el gobierno de las Tecnologías de la Información y las Comunicaciones
- Controles y objetivos de control
- Estándares y procedimientos. ISO 17799 (ISO 27002)
- Inversiones en seguridad

#### 3. Sistema de gestión de la seguridad

- Responsabilidades de la gestión de la seguridad
- La gestión integrada de la seguridad: sistema de gestión de seguridad de la información (ISO 27001)
- Métricas y cuadro integral de mando
- La organización del mando y la respuesta rápida

#### 4. Análisis de riesgos

- Metodología para el análisis y evaluación de riesgos
- Herramientas para el análisis de riesgos
- Caso práctico

#### 5. La seguridad física y del entorno

- Riesgos, amenazas y contramedidas
- El edificio
- El entorno físico del hardware: Centros de Procesos de Datos (CPD)
- Técnicas de detección, prevención y supresión de amenazas físicas
- La seguridad física del hardware

#### 6. Técnicas criptográficas

- Algoritmos criptográficos
- Aplicaciones actuales de la criptografía

#### 7. Certificación y firma electrónica

- Control de integridad
- Firma digital y firma electrónica
- Las Infraestructuras de Clave Pública (PKI)
- Tecnologías de certificación y su uso corporativo
- Principales prestadores de servicios de certificación españoles
- Normativa vigente

#### 8. Gestión de identidades y accesos

- Métodos y tecnologías de identificación
- Métodos, tecnologías y modelos de Autenticación, Autorización y Auditoría (AAA)

#### 9. La seguridad en las comunicaciones y operaciones

- Conceptos básicos de seguridad en las comunicaciones
- La seguridad en la operación de sistemas

#### 10. La seguridad en el software de base y en las aplicaciones

- Configuración y gestión de los sistemas operativos para implantar medidas de seguridad
- Diseño y desarrollo de aplicaciones informáticas seguras
- Medidas de protección contra virus y otros tipos de software malicioso
- Gestión de la seguridad en las bases de datos

#### 11. La seguridad y las personas

- Conceptos básicos relativos a la seguridad de las personas
- Controles de seguridad personal. Identificación de personas
- Concienciación y formación de la dirección y el personal

#### 12. Cumplimiento con el marco jurídico

- Marco jurídico de la Seguridad y la Auditoría de las TIC
- Privacidad y legislación sobre protección de datos

#### 13. El plan de continuidad del negocio

- Conceptos básicos
- Nociones relativas a los principales procesos. Recuperación ante desastres
- Definición e implantación de un plan de continuidad del negocio
- Respuesta ante incidentes
- Planes de contingencia
- Caso práctico

#### Proyecto fin de Máster

Orientado a la aplicación y desarrollo de los conocimientos y habilidades prácticas y de gestión impartidas en el Máster. Cada proyecto tendrá un tutor de la Universidad o ponente del curso.

## CLAUSTRO\*

El claustro está compuesto por doctores y profesionales del sector en activo.

Entre otros destacamos a:

### **D. José Luis Mancho**

Director de Tecnología de Symmetric

### **D. Emilio Castellote**

Responsable de Productos de Seguridad de Panda Security

### **D. Jesús Romero**

Director de Desarrollo de Negocio Nacional de Sistemas de Seguridad de INDRA

### **D. Marcos Gómez Hidalgo**

Subdirector de eConfianza del Instituto Nacional de Tecnologías de la Comunicación (INTECO)

### **D. Juan Salom Clotet**

Jefe del Grupo de Delitos Telemáticos de la Unidad Central Operativa de la Guardia Civil

### **D. Antonio Alcolea**

Jefe de Área de Seguridad de la Información y Confianza, Dirección General para el Desarrollo de la Sociedad de la Información del Ministerio de Industria, Turismo y Comercio

### **D. Jesús López**

Jefe de Unidad, Subdirección General de Tecnologías de Análisis de la Información e Investigación del Fraude de la Agencia Tributaria

### **D. Justo López Parra**

Responsable de Seguridad Informática y Arquitectura de Explotación de Endesa

### **D. David Villalba**

Gerente de Análisis de Incidencias, Dirección de Operaciones e Infraestructuras Corporativas de Endesa

### **D. Jesús Menéndez**

Channels Systems Engineer de CISCO

### **D. Antonio Ibáñez Meca**

Technical Account Manager de Microsoft Services

### **D. Manuel Cortés Márquez**

Security Consulting Manager de Grupo SIA

### **D. César Iglesias**

Grupo de Propiedad Intelectual y Nuevas Tecnologías de Díaz-Bastián & Truan Abogados

### **D<sup>a</sup>. Arancha Jiménez**

Responsable de Continuidad de Negocio & Risk Management de Business Consulting de Atos Consulting

### **D. José Martínez**

Jefe de Proyecto del Área de Seguridad de Business Consulting de Atos Consulting

### **D. Lucas Ocaña**

Responsable de Seguridad de Business Consulting de Atos Consulting

### **D. Luis de Salvador**

Profesor de Arquitectura de Computadores y Automática de la Universidad Europea de Madrid

### **D<sup>a</sup>. María Teresa Villalba de Benito**

Profesora de Sistemas Informáticos de la Universidad Europea de Madrid

\* La Universidad se reserva el derecho a realizar las modificaciones oportunas en el claustro propuesto.

CON LA COLABORACIÓN DE



La Universidad se reserva el derecho a retrasar el inicio del postgrado o no impartirlo si no se alcanza el número mínimo de alumnos.

La Universidad se reserva el derecho a realizar variaciones en la ubicación donde se imparte el postgrado.

**CAMPUS LA MORALEJA**  
Avda. Bruselas, 14  
28108 Alcobendas. Madrid  
Tel.: 902 23 23 50  
[www.uem.es](http://www.uem.es)



**Universidad  
Europea  
de Madrid**

Laureate International Universities